-- This session management service 24 is a service to manage the session as a unit for executing a communication processing separately from each of the information terminal 1 when a plurality of the information terminals 1 gains access to the Web server service 20 of the application server 2. --.

Rewrite the paragraph starting at page 29, line 5 and ending at page 29, line 10 as follows:

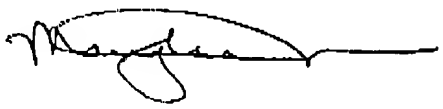
-- Furthermore, in authenticating the secret key use, justification may be determined using biometric information such as voice information (voiceprint), finger print, and retina (iris), instead of determining the justification using the passphrase applied when decrypting the secret key. --.

REMARKS

The Specification for the above-identified application has been amended to correct grammatical and typographical errors. A marked-up version of the Specification is submitted as "Attachment A - Marked-Up Version of Specification." Entry of this Preliminary Amendment is respectfully requested.

Dated: December 13, 2001

Respectfully submitted,



Marylee Jenkins
Reg. No. 37,645
An Attorney of Record

ROBIN, BLECKER & DALEY
330 Madison Avenue
New York, New York 10017
T (212) 682-9640

ATTACHMENT A - MARKED-UP VERSION OF SPECIFICATION

This is an attachment showing the marked-up version of the Specification.

In the Specification

Rewrite the paragraph starting at page 6, line 17 and ending at page 7, line 4 as follows:

-- The information terminal 1 (Personal Digital Assistant, for example), as shown in FIG. 2, comprises a CPU 51, a ROM 52, and a RAM 53. Furthermore, the information terminal 1 comprises a display device 54 consisting of a liquid crystal panel, a back light, an optical system and the like[,]. [this] This display device 54 is controlled and driven by a display control circuit 55. These CPU 51, ROM 52, RAM 53 and display control circuit 55 are connected through a CPU bus 60.

Furthermore, the CPU 51 is connected, through an I/O port, to a communication device 56 and a communication control circuit 57 for communication with an external apparatus, and an input device 58 and an input control circuit 59 for receiving instructions from a user. --.

Rewrite the paragraph starting at page 8, line 9 and ending at page 9, line 16 as follows:

-- A display service 11 is a service which displays various data on the display device 54. An input service 12 is a service which detects that a certain domain on a digitizer was pressed by a pen and the like, and provides [an] input information to various services. An

encryption communication service 13 interlocks with the Web browser service 10 and the like, and establishes an encryption communication with the application server 2.

Furthermore, as shown in FIG. 1, in the hard disk 64 of the application server 2, as a program characteristic to the present invention, a program corresponding to the following services [are] is stored.

Of these services, a Web server service 20 is a service which reads from the inside of the application server 2 and transmits [and] the like data coded with the Hypertext Markup Language (HTML) required by the Hypertext Transfer Protocol (HTTP). An encryption communication service 21 interlocks with the Web server service 20 and the like, and establishes an encryption communication (SSL and TLS, for example) with the Web browser service 10.

Furthermore, a secret key management service 22 is a service which manages, in [a] data of the Web server service 20 on the application server 2, the Web E-mail service data for example, to enable to use a secret key corresponding to a public key encryption necessary to decrypt a code applied to said E-mail data, or provide a digital signature on a created E-mail.

Further, hereupon, for the convenience of description, the public key and the secret key of the public key cryptosystem is identifiably constituted by an E-mail address used by user. Furthermore, [these] the public key and secret key always exist [in] as a pair as the one and only key. --.

Rewrite the paragraph starting at page 11, line 2 and ending at page 11, line 9, as follows:

-- FIG. 8 is a diagram showing an example of the window of the information terminal 1 in the case where a new E-mail is created, after the access by the Web browser service 10 of the information terminal 1 to the Web E-mail service 23 on the Web server service 20 of the application server 2 is succeeded, and the access to the allowance authentication for use of the secret key is also succeeded. --.

Rewrite the paragraph starting at page 11, line 15 and ending at 12, line 7 as follows:

-- FIGs. 10 to 11 indicate a flowchart showing a processing of the information terminal 1 in the first embodiment of the present invention. FIG. 12 is a flowchart showing a processing of the application server 2 in the first embodiment of the present invention. FIG. 13 is a flowchart continued from FIG. 12. FIG. 14 is a flowchart showing a signature processing in the information terminal 1, and FIG. 15 is a flowchart showing a signature processing in the application server 2.

Next, [processings] the processing characteristic to the present invention will be described in detail according to the flowcharts of FIGs. 10 to 15.

First, by the browser service 10 of the information terminal 1, an address Uniform Resource [Locators] Locator (URL) or Uniform Resource [Indicators] Indicator (URI) is inputted and transmitted through an input service 12 (step S1010 of FIG. 10). As an input method of the input service 12, a software keyboard and the like can be cited. --.

Rewrite the paragraph starting at page 12, line 26 and ending at page 14, line 5 as follows:

-- As a result, in the case where the received application server authentication is not acceptable to said information terminal 1, a message to the effect that the establishment of the encryption Web communication is rejected is transmitted to the application server 2 (step S1050 of FIG. 10). The encryption communication service 21 of the application server 2, upon receiving the message to the effect that the establishment of the encryption Web communication is rejected, transmits [a] display data showing non-establishment of the encryption Web communication to the information terminal 1, and ends the operation (step S1060 of FIG. 12). The Web browser service 10 of the information terminal 1 displays the received display data showing non-establishment of the encryption Web communication, and ends the operation (step S1070 of FIG. 10).

In the case where the received application server authentication is acceptable to said information terminal 1, a message to the effect that the establishment of the encryption Web communication is transmitted to the application server 2 (step S1080 of FIG. 10). The encryption communication service 21, upon receiving a message to the effect that the establishment of the encryption Web communication is acceptable, exchanges [a] the remaining information necessary for the encryption Web communication with the encryption communication service 13, thereby to establish the encryption Web communication, starts a session program (hereafter referred to as a session) dedicated to perform [an] encryption communication processing with said information terminal 1, and causes said session to manage the processing of the encryption data communication with said information terminal 1. --.

Rewrite the paragraph starting at page 14, line 15 and ending at page 15, line 4 as follows:

-- Further, in the present invention, allowance for use of the secret key is authenticated using the encryption Web communication continuously established between the information terminal 1 and the application server 2 as a unit, in the case the session is closed, that is, in the case where the encryption Web communication established between a certain information terminal 1 and the application server 2 is closed, allowance of the authentication for use of the secret key is also cancelled simultaneously, as will be stated later.

After the encryption Web communication is established, the Web server service 20 of the application server 2 transmits [an] access window data to the Web E-mail service 23 required by the information terminal 1 in the step S1010 of FIG. 10, to the information terminal 1 (step S1090 of FIG. 12). --.

Rewrite the paragraph starting at page 15, line 21 and ending at page 15, line 27 as follows:

-- The Web server service 20 of the application server 2, upon receiving the input data such as the display data, user ID and password (step S1120 of FIG. 12), judges whether the received user ID and password are the user ID and the password registered in the application server 2 as the correct data accessible to the Web E-mail service 23 (step S1130 of FIG. 12). --.

Rewrite the paragraph starting at page 17, line 26 and ending at page 18, line 5 as follows:

-- As a result, in the case where the use of the secret key is allowed in the present session, that is, in the case where the present session continues as the session where the use is allowed once, the program proceeds to a step S1320 of FIG. 13. Furthermore, whether or not the same session is judged by an identifier such as a session number is determined. --.

Rewrite the paragraph starting at page 19, line 17 and ending at page 20, line 16 as follows:

-- As a result, if the passphrase is [a] fail data, the Web E-mail service 23 transmits a message window data to the effect that the passphrase is [a] fail data to the information terminal 1 through the Web server service 20 (step S1290 of FIG. 13), ends a passphrase processing, and returns to a condition before the decryption software button 105 is pressed. The Web browser service 10 of the information terminal 1, upon receiving the message window data to the effect that the passphrase is [a] fail data (step S1300 of FIG. 11), analyzes such data, and displays by the display server 11 (step S1310 of FIG. 11).

In the case where the passphrase is correct, the Web E-mail service 23 decrypts the secret key allowed for use of a copy of E-mail concerning a decryption request (step S1320 of FIG. 13), and transmits [a] display shape change data of a decryption software button 112 and a signature software button 113 to the Web browser service 10 of the information terminal 1 through the Web server service 20 (step S1330 of FIG. 13). Furthermore, the display shape change data of the decryption software button 112 and the signature software button 113 is transmitted to indicate that the allowance for use of the secret key is obtained

in the present session, and this secret key use allowance information is saved until said session is closed as [an] additional information of the present session. --.

Rewrite the paragraph starting at page 21, line 2 and ending at page 21, line 8 as follows:

-- Next, in the Web server service 20 of the application server 2, there is a session which controls [a] dialogue processing and the like with the information terminal 1, in the case where the secret key use allowance of the user of the information terminal 1 is retained, procedures for processing the digital signature to the created E-mail are described. --.

Rewrite the paragraph starting at page 21, line 18 and ending at page 21, line 26 as follows:

-- The Web E-mail service 23 of the application server 2, upon receiving the information of the press down of the E-mail generation software button 114 and the display data of FIG. 7 through the Web server service 20 (step S1410 of FIG. 15), transmits [an] E-mail creation window data and [a] creation software highlight data to the Web browser service 10 of the information terminal 1 through the Web server service 20 (step S1420 of FIG. 15). --.

Rewrite the paragraph starting at page 22, line 21 and ending at page 23, line 15 as follows:

-- The Web E-mail service 23 of the application server 2, upon receiving the press down information of the signature software button 113 and the display data of FIG. 8

through the Web server service 20 (step S1460 of FIG. 15), inquires to the secret key management service 22 as to whether [own] the known session retains the secret key use allowance (step S1470 of FIG. 15).

As a result, in the case where the [own] known session does not retain the secret key use allowance, the same processing as the steps S1240, S1270, and S1280 of FIG. 13 is executed (step S1480 of FIG. 15).

In the case where the [own] known session retains the secret key use allowance, the Web E-mail service 23 of the application server 2 causes the secret key management service 22 to execute a digital signature on a document of an E-mail concerning receiving and creation using the secret key concerning the use allowance of the above (step S1490 of FIG. 15), and transmits the display window data of the contents of the E-mail executed by the digital signature to the Web browser service 10 the information terminal 1 through the Web server service 20 (step S1500 of FIG. 15). --.

Rewrite the paragraph starting at page 24, line 22 and ending at page 25, line 27 as follows:

-- This session management service 24 is a service to manage the session as a unit for executing a communication processing separately from each of the information terminal 1 when a plurality of the information [terminal] terminals 1 gains access to the Web server service 20 of the application server 2. --.

Rewrite the paragraph starting at page 29, line 5 and ending at page 29, line 10 as follows:

-- Furthermore, in authenticating the secret key use, justification may be determined using [a] biometric information such as voice information (voiceprint), finger print, and retina (iris), instead of determining the justification using the passphrase applied when decrypting the secret key. --.